논문 13-38A-11-06

한국통신학회논문지(J-KICS) '13-11 Vol.38A No.11
http://dx.doi.org/10.7840/kics.2013.38A.11.967

클라우드 스토리지의 공유 데이터에 대한 효율적 다중 서명 기법

김 영 식•

An Efficient Multi-Signature Scheme for Shared Data in a Cloud Storage

Young-Sik Kim•

요 약

이 논문에서는 클라우드에서 공유된 데이터에 대한 겹선형 사상 기반의 효율적인 다중 서명 방법을 제안하고, 계산적 DH (computational Diffie-Hellman) 문제의 어려움에 기반을 둔 보안 특성을 증명한다. 제안하는 방법은 서명 검증하는 단계에서 전체 데이터를 다운로드하는 대신 클라우드 서버가 제공하는 데이터 블록의 해쉬 값의 합을 이용함으로써 검증에 필요한 다운로드 데이터 크기를 작게 하였다.

Key Words : multi-signature, cloud, multi-owner, integrity, bilinear mapping

ABSTRACT

In this paper, we propose an efficient mult-signature scheme based on a bilinear mapping for shared data in the cloud and prove the security of the proposed scheme using the difficulty of the computational Diffie-Hellman problem. For verification, the scheme is using the sum of the hash values of stored data rather than the entire data, which makes it feasible to reduce the size of the downloaded data.

Ⅰ. 서 론

오늘날 클라우드 컴퓨팅은 자원을 공유로 저 비용의 컴퓨팅 환경이 가능하게 만들어 주며, 여러 사용자간에 편리한 공유 환경을 제공하여 공동 작업 및 업무 분담의 효율성을 높일 수 있다.

사용자간 데이터 공유를 위해서는 저장된 데이터에 대한 안정적이고 신뢰성 있는 환경이 반드시 요구된다. 기존의 관련된 보안 연구들은 대부분 저장된 데이터의 동적인 데이터 연산 및 데이터 프라이버시에 초점을 두고 이루어졌다[1-3].

최근에는 프라이버시를 제공하면서 정당한 사용자 중 한 사람이 공유된 데이터에 대한 독립적으로 무결성을 검증하는 메커니즘들에 대한 연구들이 이루어졌다[4,5]. 이런 연구들에서 저장된 데이터의 각 블록이 독립적으로 처리되기 때문에, 사실상 각 블록별로 단일 소유자에 대한 검증 서비스를 제공하는 것과 같다. 이 때 다중 서명을 이용할 수 있지만[6], 데이터를 검증하는 단계에서 클라우드 서버에 저장된 모든 데이터를 불러와서 다시 연산을 수행해야하는 문제가 발생한다.

이 논문에서는 클라우드에서 공유된 데이터에 대한 효율적인 겹선형 사상 기반의 다중 서명 방법을 제안하며 계산적 DH (computational Diffie-Hellman)문제의 어려움에 기반을 둔 보안 특성을 증명할 것이다. 제안하는 방식은 서명을 검증하는 단계에서 검증에 필요한 다운로드 데이터를 줄일 수 있고, 제3의 검증 서비스 제공자가 공개된 데이터로 효율적 검증이 가능한 방식이다.

Ⅱ. 시스템 모델 및 배경 지식

2.1. 시스템 모델

제안 하는 방식에서는 다중 소유자, 클라우드 서버, 그리고 공개 검증자가 존재한다. 여러 사용자가 공유하는 데이터는 여러 블록으로 나누어지고 각 블록에 대해서 모든 소유자들이 서명을 하게 된다. 모든 사용자의 서명이 문제가 없을 때만 다중 소유 데이터의 무결성에 문제가 없는 것으로 간주된다.

2.2. 암호학적 도구

본 논문에서 제시하는 서명 방식은 겹선형 사상에 기반을 두고 있는데, 다음과 같이 정의된다. 먼저 G_1과 G_2가 차수가 소수 p인 두 개의 곱셈 순회 군이고, g가 G_1의 생성자라 하자. 그러면 이중 선형 사상 e: $G_1 \times G_1 \rightarrow G_2$ 는 다음과 같은 성질을

※ 본 연구는 한국연구재단 중견핵심연구과제(NRF-2011-0016664) 지원으로 수행되었습니다.
• First Author조선대학교 정보통신공학과 정보이론 및 보안 연구실, iamyskim@chosun.ac.kr, 정회원
논문번호 : KICS2013-10-438, 접수일자 : 2013년 10월 10일, 최종논문접수일자 : 2013년 10월 28일

갖는다.

1) 계산가능성: 모든 $u,v\in G_1$ 에 대하여, $e(u,v)$ 를 계산하는 효율적인 알고리즘이 존재한다.
2) 이중 선형성: 모든 $u,v\in G_1$ 과 $a,b\in Z_p$ 에 대해서 $e(u^a,v^b)=e(u,v)^{ab}$
3) Non-degeneracy: $e(u,u)\neq 1$

Ⅲ. 클라우드 환경에서의 새로운 다중 사용자의 다중 서명 방식

제안하는 방식에서 다중 서명을 위해 사용되는 파라미터는 $P=(e,p,G_1,G_2,g,H)$ 로 나타낼 수 있다. 여기에서 $H:\{0,1\}^*\rightarrow Z_p$ 인 해쉬 함수이다. 다중 소유자의 총수를 N이라 하자. 데이터 M은 총 k개의 블록으로 나누어지고 그 값을 $M=m_1\|m_2\|\cdots\|m_k$ 라 하자. 그리고 다중 소유자를 $S=\{S_1,S_2,\cdots,S_N\}$ 로 나타내자. 그러면 제안하는 다중 서명은 네 단계로 이루어진다.

1) 키 생성 단계: $KG(P)\rightarrow(sk,pk)$

파라미터 P가 주어져 있을 때 i번째 사용자 S_i는 Z_p의 원소 중에서 랜덤하게 선택한 x_i를 자신의 비밀키 $sk_i=x_i$ 로 하고 이에 대응되는 공개키 $pk_i=g^{x_i}\in G_1$ 를 계산한다.

2) 서명 단계: $Sign(m_i,ID_i,\{pk_1,\cdots,pk_N\})$

서명하고자 하는 i번째 $(1\le i\le k)$ 메시지 블록을 m_i이라 하고 메시지의 identifier를 ID_i 라 하자. 그러면 사용자 S_j는 데이터와 ID_i의 해쉬 값 $h_i=H(ID_i\|m_i)\in Z_p$ 를 계산한 후에 다시 비밀키 x_j를 이용해서 $s_{ji}=g^{h_ix_j}$를 계산하여 클라우드 서버로 s_{ji}를 전송한다. 각 사용자가 계산한 i번째 데이터 m_i에 대한 N개의 서명이 모두 클라우드 서버에 도착하면, 클라우드 서버는 모든 소유자의 서명의 G_1 상에서의 곱 $s_i=\prod_{j=1}^{N}s_{ji}$를 해당 블록의 다중 서명 값으로 계산하여 서버에 저장한다.

3) 대표 값 생성 단계:

$RepresentGen(M,\{s_1,\cdots,s_k\})\rightarrow(\gamma,\sigma)$

수집된 서명을 이용해서 클라우드 서버는 저장된 데이터의 대표 값과 대표 서명을 생성한다. 이 때 대표 데이터 값은 $\gamma=\sum_{i=1}^{k}h_i \bmod p\in Z_p$ 이고, 대표 서명 값은 $\sigma=\prod_{i=1}^{k}s_i\in G_1$ 이다. 이 두 개의 값이 서버에 저장된다.

4) 검증 단계: $Verify(M,ID,\{pk_1,\cdots,pk_N\},s)$

메시지 블록, 해당 블록의 ID, 그리고 공개키 및 서명 값이 주어져 있을 때, $e(\sigma,g)=e(g^{\gamma},pk)$ 가 성립하면 검증이 된 것으로 판단하고 그렇지 않으면 검증되지 않은 것으로 판단한다. 여기에서 pk는 사용자의 모든 공개키 pk_i들의 G_1에서의 곱셈이다. 즉, $pk=\prod_{i=1}^{N}pk_i\in G_1$ 이다.

검증 단계의 유효성은 다음과 같이 이중 선형성에 의해서 확인이 가능하다.

$$\begin{aligned}e(\sigma,g)&=e\left(\prod_{i=1}^{k}\prod_{j=1}^{N}s_{ji},g\right)=e\left(\prod_{i=1}^{k}\prod_{j=1}^{N}(g^{h_ix_j}),g\right)\\&=e\left(g^{\sum_{i=1}^{k}h_i\sum_{j=1}^{N}x_j},g\right)=e\left(g^{\gamma},g^{\sum_{j=1}^{N}x_j}\right)\\&=e\left(g^{\gamma},\prod_{j=1}^{N}g^{x_j}\right)=e(g^{\gamma},pk)\end{aligned}$$

Ⅳ. 보안 분석

제안하는 방식의 보안 특성 증명을 위해 다음과 같이 계산적 DH (CDH) 가정을 정의할 필요가 있다.

정의 1. $a,b\in Z_p^*$ 인 원소에 대해 $g,g^a,g^b\in G_1$ 가 임의의 확률적 다항식 시간 공격자 A_{CDH}의 입력으로 주어진다고 하자. 이 공격자가 출력 $g^{ab}\in G_1$ 을 얻는 것은 계산적으로 불가능하고 이것은 다음과 같이 나타낼 수 있다.

$$\Pr[A_{CDH}(g,g^a,g^b)=<g^{ab}>:a,b\xleftarrow{R}Z_p^*]\le\epsilon$$

그러면 다음과 같이 제안하는 보안 특성을 증명할 수 있다.

정리 2. 공격자가 제안하는 방식의 위조 서명을 생성하는 것은 계산적으로 불가능하다.

증명) 다중 서명의 경우에는 $N-1$명의 사용자의 비밀키 값을 알고, 마지막 한 명의 비밀키만 몰라도 위조가 계산적으로 불가능해야한다[6]. 먼저 공격자가 모든 메시지 $M=m_1\|\cdots\|m_k$ 와 대응되는 ID_i $(1\le i\le k)$를 모두 알고 있다고 가정하자. 그리고

i번째 메시지 블록 m_i에 대해서, 공격자가 두 번째에서 N번째 사용자의 비밀키 $x_2,\cdots,x_N$을 알아냈다고 하자. 이 때 메시지 m_i와 ID_i는 공개되어 있으므로, 해쉬값 $h_i = H(ID_i \| m_i)$는 쉽게 계산 가능하다. 그러면 메시지 m_i에 대한 다중 서명 s_i는 다음과 같다.

$$s_i = \prod_{j=1}^{N} s_{ji} = \prod_{j=1}^{N} g^{h_i x_j} = g^{h_i x_1}\left(\prod_{j=2}^{N} g^{x_j}\right)^{h_i}$$

다시 대표 서명은 다음과 같이 나타낼 수 있다.

$$\sigma = \prod_{i=1}^{k} s_i = \prod_{i=1}^{k} g^{h_i x_1}\left(\prod_{j=2}^{N} g^{x_j}\right)^{h_i}$$
$$= g^{x_1 \sum_{i=1}^{k} h_i} g^{\sum_{j=2}^{N} x_j \sum_{i=1}^{k} h_i} = g^{\gamma x_1} g^{\gamma x'}$$

가 된다. 단, $x' = \sum_{j=2}^{N} x_j$이다. 즉, 만일 공격자가 서명을 위조해 유효한 σ^*를 얻었다면, 이것은 위조된 서명으로부터 다음 계산이 가능함을 의미한다.

$$\sigma^* = g^{\gamma x} g^{\gamma x_1^*} \Rightarrow g^{\gamma x_1^*} = \sigma^* / g^{\gamma x}$$

즉, $g, g^{x_1^*}, g^{\gamma}$ 가 주어져 있을 때 $g^{\gamma x_1^*}$를 계산한 것이 되어 CDH 문제를 푼 것이 된다. 반대로, CDH 문제가 계산적으로 불가능하면 제안하는 다중 서명 방식을 위조하는 것도 계산적으로 불가능하다.

Ⅴ. 성능 비교

Stanford의 Pairing Based Cryptography (PBC) library를 이용해서 제안하는 방식에서 사용하는 겹선형 사상을 구현하였고, 이 때 MNT curve에 기저체의 크기는 159비트를 이용하였다[7]. 모든 실험은 3세대 Core i7 2.7GHz 쿼드 코어 프로세서에 8GB 1600 MHz DDR3 메모리를 사용하는 환경에서 이루어졌다. 사용하는 데이터의 블록의 수는 k = 1,000,000개이고 각 블록의 크기는 1,024비트이며, 그룹의 차수인 p는 크기가 160비트이고 사용자 수 $N=5$를 이용하였다. 비교를 위해 기존에 널리 사용되는 서명 방식을 사용하였다[8].

표 1. 성능 비교를 위한 시뮬레이션 결과
Table 1. Simulation results for performance comparison

	Previous[8]	Proposed
Verification Time (s)	140.73	28.15
Transmitted data (KB)	640	100

그 결과 표 1과 같이 제안하는 방식이 기존의 표준적인 클라우드상의 전자서명 방식에[8] 비해서 약 5배가량 더 성능이 향상되었고, 다운로드 데이터도 약 15.6%로 줄어든 것을 확인하였다.

Ⅵ. 결 론

이 논문에서는 클라우드에서 공유된 데이터에 대한 효율적인 겹선형 사상 기반의 다중 서명 방법을 제안하였고, CDH 문제의 어려움에 기반을 둔 보안 특성을 증명하였다. 제안하는 방식은 서명을 검증하는 단계검증에 필요한 데이터 크기를 크게 줄여 효율적 검증이 가능하게 해 준다.

References

[1] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, “LT codes-based secure and reliable cloud storage service,” in *Proc. IEEE INFOCOM 2012*, pp. 693-701, Orlando, U.S.A., Mar. 2012.

[2] A. Juels and A. Oprea, “New approaches to security and availability for cloud data,” *Commun. ACM*, vol. 56, no. 2, pp. 64-73, Feb. 2013.

[3] I. Y. Jung, I. Jo, and Y. Yu, “Trust assurance of data in cloud computing environment,” *J. KICS*, vol. 36, no. 9, pp. 1066-1072, Sep. 2011.

[4] B. Wang, B. Li, and H. Li, “Public auditing for shared data with efficient user revocation in the cloud,” in *Proc. IEEE INFOCOM 2013*, pp. 2904-2912, Turin, Italy, Apr. 2013.

[5] B. Wang, H. Li, and M. Li, “Privacy-preserving public auditing for shared cloud data supporting group dynamics,” in *Proc. IEEE ICC 2013*, pp. 539-543, Budapest, Hungary, June 2013.

[6] M. Bellare and G. Neven, “Identity-based multi-signatures from RSA,” in *Proc. Cryptographers’ Track at the RSA Conf. (CT-RSA 2007)*, pp. 145-162, San Francisco, U.S.A., Feb. 2007.

[7] *Pairing Based Cryptography (PBC) library*, retrieved June 14, 2013, from http://crypto.stanford.edu/pbc/.

[8] H. Shacham and B. Waters, “Compact proofs of retrievability,” in *Proc. ASIACRYPT 2008*, pp. 90-107, Melbourne, Australia, Dec. 2008.